

Utiliser Qualys dans un environnement décentralisé:

De l'utilité d'un tableau de bord unifié et personnalisé

Guillaume Kermarrec & Laurent Bourhis
Direction de la Sûreté Veolia





A propos de Veolia



25 125 M€
CA en 2017

169 000
employés en 2017



Veolia conçoit et déploie des solutions de **gestion de l'eau**, **des déchets** et de l'**énergie**, participant au développement durable des villes et des industries.



Gestion du cycle global de l'eau,
de la production et de la distribution d'eau potable à la collecte, au traitement et au recyclage des eaux usées.



Liquide et solide non dangereux et dangereux gestion des déchets
Notre expertise couvre l'ensemble du cycle de vie des déchets, de la collecte au recyclage. à la valorisation finale des déchets en matériaux ou en énergie



Efficacité énergétique, gestion efficace des réseaux de chauffage et de refroidissement,
la production d’énergie verte à la valorisation finale des déchets sous forme de matériaux ou d’énergie

Evolution IT de Veolia



SECURITY

VEOLIA

G Suite
Migration program

90,000 users
2,000 video meetings/mth
5M docs in Drive
6,000 Mngd Mobile

amazon web services

140,000 users
90,000 video meetings/mth
100M docs in Drive
60,000 Mngd Mobiles
5,000 Chromebooks

#DataCenterLess
#SecurebyDesign
Full Agile
Full Chromebook
Full Web & Mobile

SATAWAD UP to collaboration and beyond

Digital

Prerequisite

3 Public Cloud platforms & contracts

10%

Experiment

New culture:
Agile, Measure
Product Adoption
DevSecOps, FinOps

25%

Go agile

1st Digital
Delivery Team with
developers,
Cloud experts,
Data scientists

Internal Marketplace

50%

Agile@scale

90%

Product oriented, Digital adoption measure
Digital Factory >100 headcount
Digital talent programs
Digital Ambassadors & Global Digital community

+250 messaging systems
12,000 servers
in +50 data centers
80,000 PCs

2012 2013 2014 2015 2016 2017 2018 2020

Les missions de la cybersécurité Veolia



7 missions de la cybersécurité Veolia

1. **Identifier les risques et les menaces cyber**
2. Prévenir l'apparition d'incidents
3. Développer la formation des utilisateurs
4. **Monitorer la sécurité des SI**
5. Gérer les incidents et crises de cybersécurité
6. Développer des plans de continuité et de secours
7. **Suivre l'évolution des menaces et des vulnérabilités**



L’organisation cybersécurité Veolia



- Président Veolia
- Secrétaire Général Veolia
- Directeur de la Sûreté Veolia
- Directeur Informatique Veolia
- Directeur de la Cybersécurité Veolia

Eau France | Propreté France | UK + IE | Europe du Nord | Europe Centrale | Asie | Amérique du Nord | AU/NZ | Afrique & Moyen Orient | LATAM | Entreprise s Globales | Corporate & Groupe

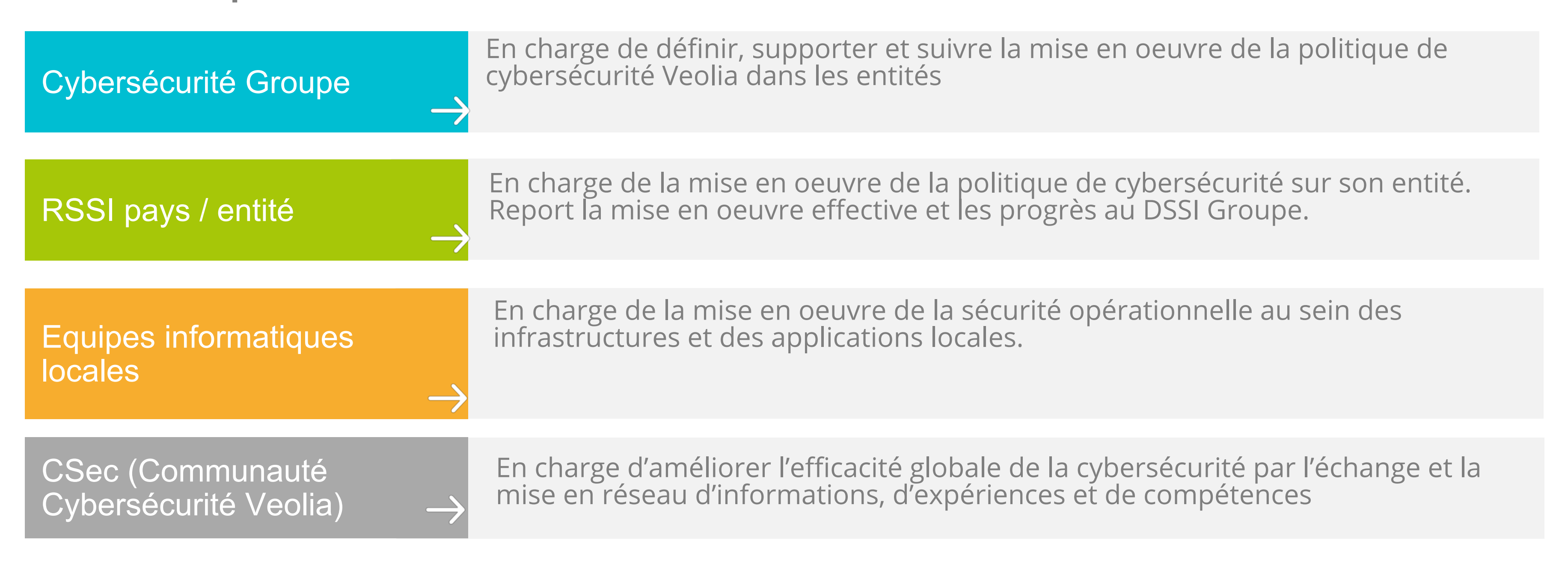
L’organisation cybersécurité Veolia



L’organisation cybersécurité Veolia



Qui fait quoi ?



Service de scan de vulnérabilités Veolia



Scans externes de vulnérabilité

Scan mensuel de toutes les infrastructures Veolia exposées sur Internet.
Environ 2000 systèmes dans plus de 30 pays.
Suivi des vulnérabilités et des plans d'actions

Global trend vulnerability evolution through the year

Total
20.00%
15.00%
10.00%
5.00%
0.00%
Sept Oct Nov Dec Jan Feb Mar Apr May June July Aug Sept Oct Dec April May June July Aug

Scans internes de vulnérabilité

Disponible sur demande du RSSI de l'entité
Coût des licences pris en charge par l'équipe cybersécurité Groupe
Autonomie des équipes locales pour gérer les scans



July		Severities		Vulnerable Hosts		Vulnerable Hosts			Vulnerability Type		Vulnerability Status			
Zone	Scanned Last 30 days	L5	L4	L5	L4	Last 30 days	Ratio %		Confirmed	Potential	New	Active	FixedLast 30 days	RO
A	175	0	26	0	10	10	5.7%	▲	4	22	5	18	1	3
B	31	1	1	1	1	2	6.5%	▲	2	0	0	2	0	0
C	267	37	187	24	39	47	17.6%	▼	29	195	12	200	23	12
D	26	5	1	5	1	6	23.1%	▲	6	0	0	6	1	0
E	75	4	28	4	11	12	16.0%	▲	4	28	0	31	1	1
F	40	0	3	0	3	3	7.5%	▼	3	0	0	0	0	3
G	678	29	160	21	50	55	8.1%	▼	37	152	30	142	26	17
H	46	9	53	9	7	14	30.4%	▲	6	56	0	59	0	3
I	46	2	10	2	3	4	8.7%	▼	1	11	0	12	1	0
J	252	14	33	13	12	24	9.5%	▲	14	33	1	44	3	2
K	154	3	12	2	6	8	5.2%	▲	2	13	3	12	16	0
L	139	15	16	7	7	10	7.2%	▼	12	19	0	31	2	0
M	56	0	0	0	0	0	0.0%	▼	0	0	0	0	0	0
Total	**1985**	**119**	**530**	**88**	**150**	**195**	**9.8%**	▼	**120**	**529**	**51**	**557**	**74**	**41**
July	**2101**	**129**	**557**	**92**	**164**	**212**	**10.09%**							
Difference	**-5.8%**	**-8.4%**	**-5.1%**	**-4.5%**	**-9.3%**	**-8.7%**	**-2.7%**							

Des besoins attendus et identifiés



- Proposer une interface simple et synthétique avec les informations collectées
- Identifier rapidement les serveurs vulnérables à mettre à jour et/ou à isoler
- Identifier des points de vigilance et des vulnérabilité de notre SI
- Avoir un impact fort auprès des DSI, RSSI & directeurs de zones/ business units

Quelques données clés



Organisation & gouvernance



- Un RSSI rattaché à la Direction Informatique
- Temps plein ou partiel suivant la taille et les enjeux
- Une équipe cybersécurité dans les grandes entités

Postes de travail & serveurs





- 11 500 serveurs
- 74 000 postes de travail
- Répartition mondiale

Budget





- Suivant le taille de l'entité et des risques locaux
- Entre 2 et 10% du budget IT local (moyenne Veolia 4,6%)

Data center



- AWS
- GCP
- Privés (fermeture fin 2019)





Chiffres clés sur la configuration de Qualys

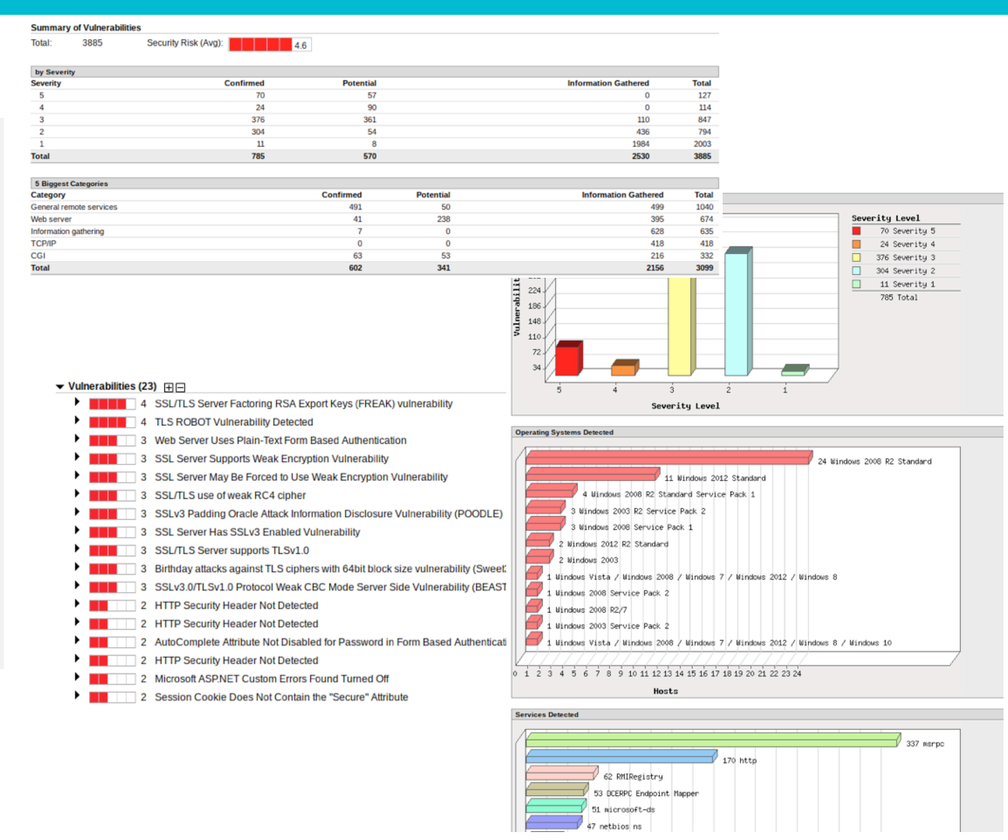


IP scannées	~ 7 000 IP scannées au niveau groupe (dont ~2 000 IP publiques) & ~ 4 000 IP scannées de manière décentralisée
Organisation	Découpage par unité organisationnelle (OU) 122 utilisateurs VM & CA
Droits d'accès	Gestion des droits par Business unit (BU) Activation de la 2FA obligatoire
ThreatProtect	Activation de ThreatProtect sur toutes les IP externes Veille active sur les alertes
Scans	Scans mensuel sur les IP externes fait par le groupe Scans interne gérés par les entités
Outils utilisés	VM AssetView CloudView ThreatProtect CloudAgent (serveurs critiques)
Administration	Administration de la plateforme au niveau groupe

Processus de communication actuel & bilan



- Des rapports mensuels fournis aux correspondants RSSI pour les IP externes
- Une mise en action poussive pour corriger les vulnérabilités
- Manque de visibilité pour le management avec une vue trop technique



Summary of Vulnerabilities

Total: 3885 Security Risk (Avg): 4.6

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	70	57	0	127
4	24	90	0	114
3	376	361	110	847
2	304	54	436	794
1	11	8	1984	2003
Total	**785**	**570**	**2530**	**3885**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	491	50	499	1040
Web server	41	238	395	674
Information gathering	7	0	628	635
TCP/IP	0	0	418	418
CGI	63	53	216	332
Total	**602**	**341**	**2156**	**3099**

Vulnerabilities (23)

- 4 SSL/TLS Server Factoring RSA Export Keys (FREAK) vulnerability
- 4 TLS ROBOT Vulnerability Detected
- 3 Web Server Uses Plain-Text Form Based Authentication
- 3 SSL Server Supports Weak Encryption Vulnerability
- 3 SSL Server May Be Forced to Use Weak Encryption Vulnerability
- 3 SSL/TLS use of weak RC4 cipher
- 3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)
- 3 SSL Server Has SSLv3 Enabled Vulnerability
- 3 SSL/TLS Server supports TLSv1.0
- 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet
- 3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST
- 2 HTTP Security Header Not Detected
- 2 HTTP Security Header Not Detected
- 2 AutoComplete Attribute Not Disabled for Password in Form Based Authenticati
- 2 HTTP Security Header Not Detected
- 2 Microsoft ASP.NET Custom Errors Found Turned Off
- 2 Session Cookie Does Not Contain the "Secure" Attribute

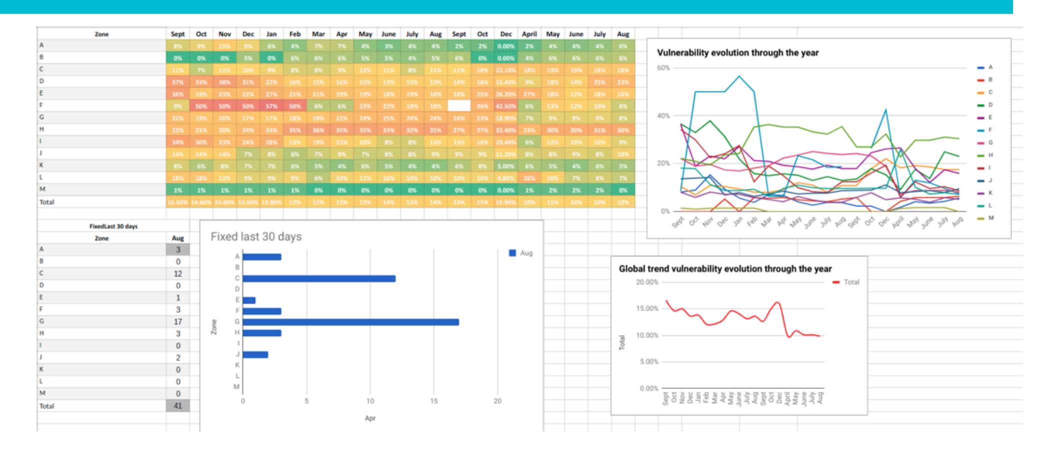
Les synthèses mensuelles

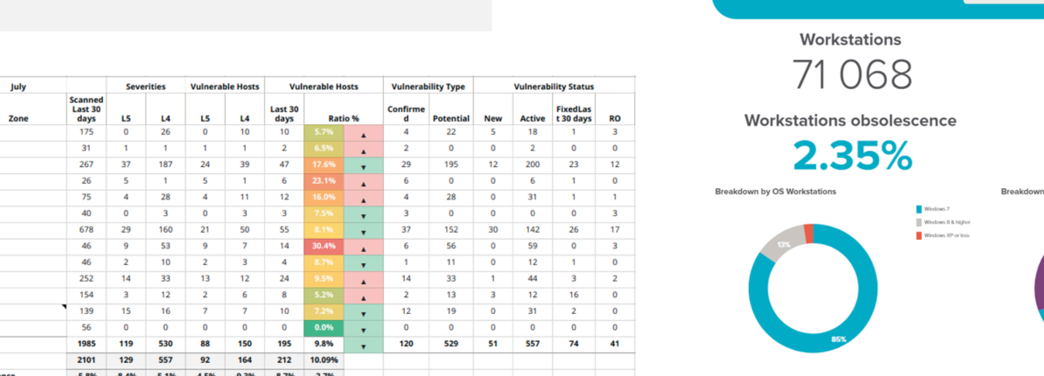


→ Information éparpillée, peu synthétique et sans contexte

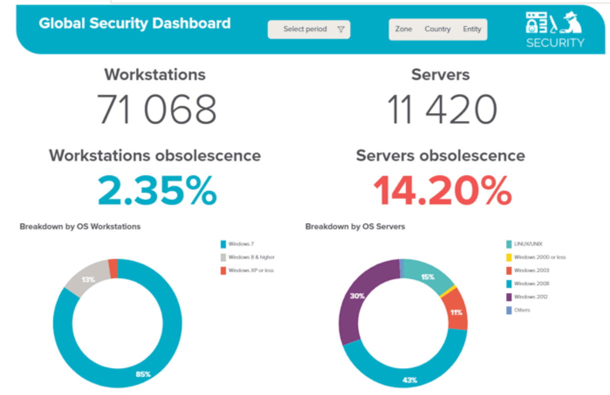
→ Faible utilisation et donc peu d'impact auprès des DSI & directeurs de zones/BU

→ Solutions non unifiées





July		Severities		Vulnerable Hosts		Vulnerable Hosts			Vulnerability Type		Vulnerability Status			
Zone	Scanned Last 30 days	L5	L4	L5	L4	Last 30 days	Ratio %		Confirmed	Potential	New	Active	FixedLast 30 days	RO
A	175	0	26	0	10	10	5.7%	▲	4	22	5	18	1	3
B	31	1	1	1	1	2	6.5%	▲	2	0	0	2	0	0
C	267	37	187	24	39	47	17.6%	▼	29	195	12	200	23	12
D	26	5	1	5	1	6	23.1%	▲	6	0	0	6	1	0
E	75	4	28	4	11	12	16.0%	▲	4	28	0	31	1	1
F	40	0	3	0	3	3	7.5%	▼	3	0	0	0	0	3
G	678	29	160	21	50	55	8.1%	▼	37	152	30	142	26	17
H	46	9	53	9	7	14	30.4%	▲	6	56	0	59	0	3
I	46	2	10	2	3	4	8.7%	▼	1	11	0	12	1	0
J	252	14	33	13	12	24	9.5%	▲	14	33	1	44	3	2
K	154	3	12	2	6	8	5.2%	▲	2	13	3	12	16	0
L	139	15	16	7	7	10	7.2%	▼	12	19	0	31	2	0
M	56	0	0	0	0	0	0.0%	▼	0	0	0	0	0	0
Total	**1985**	**119**	**530**	**88**	**150**	**195**	**9.8%**	▼	**120**	**529**	**51**	**557**	**74**	**41**
July	**2101**	**129**	**557**	**92**	**164**	**212**	**10.09%**							
Difference	**-5.8%**	**-8.4%**	**-5.1%**	**-4.5%**	**-9.3%**	**-8.7%**	**-2.7%**							



Quelles sont nos problématiques ?



- Comment améliorer la visibilité aux directions et aux équipes ?
- Comment faciliter et améliorer la visibilité des vulnérabilités à corriger ?
- Comment gérer l'identité de l'utilisateur et filtrer les données visibles ?
- Comment faciliter l'intégration des assets Amazon

Solution proposée



Dashboard accessible en ligne et scalable en fonction du besoin

Une mise à jour automatisée via l'API et une consolidation des KPI

Impact important dans les comités de pilotage

Une gestion des accès et des filtrage réalisés via SSO







Fonctions de découvertes - Connecteurs AWS







Vérification des politiques appliquées sur AWS **CloudView**

Découverte automatisée des instances AWS **AssetView**



Scan interne & externe de nos instances AWS (EC2 & ELB) **VM**



Scan externe de nos instances EC2 **CloudPerimeter**

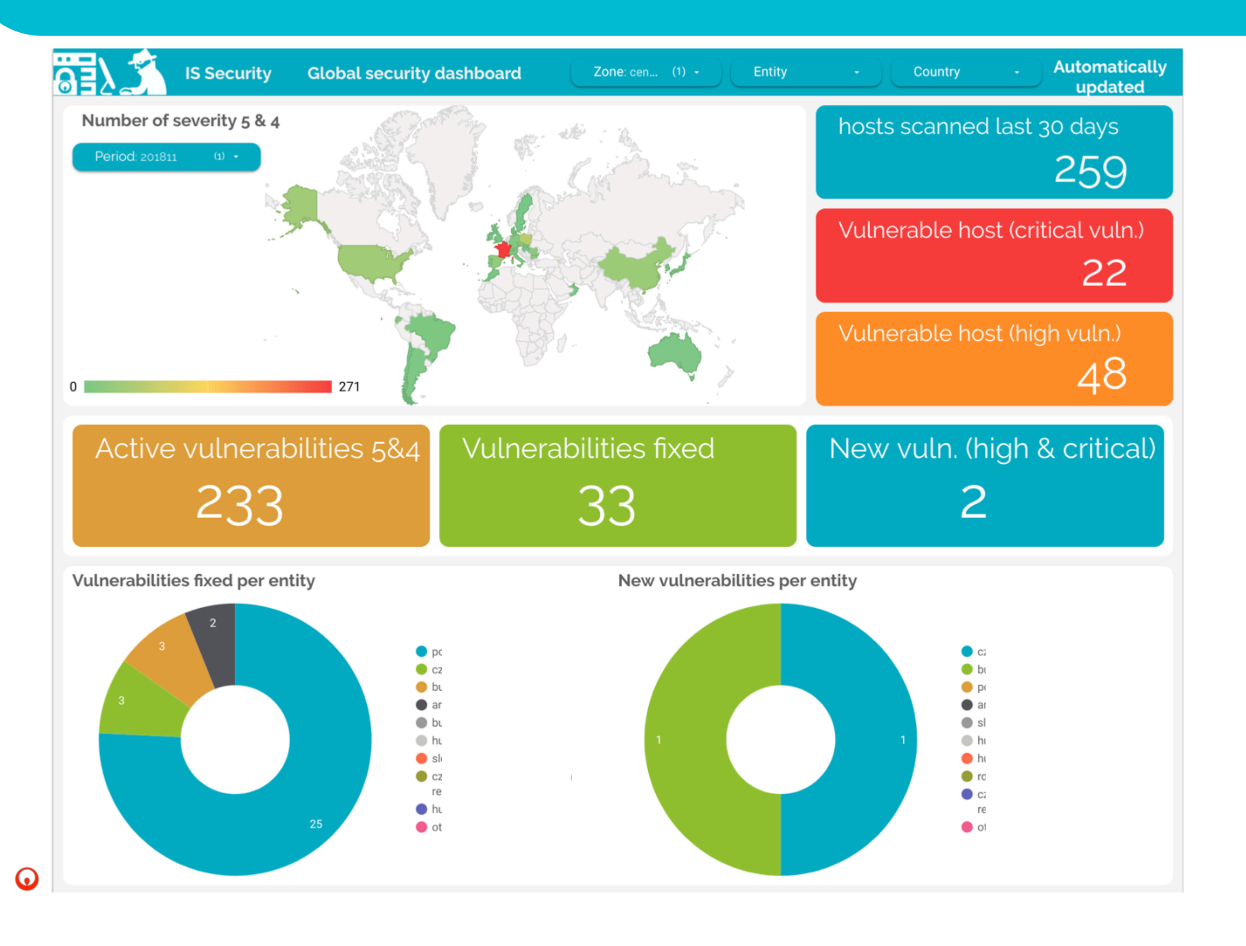


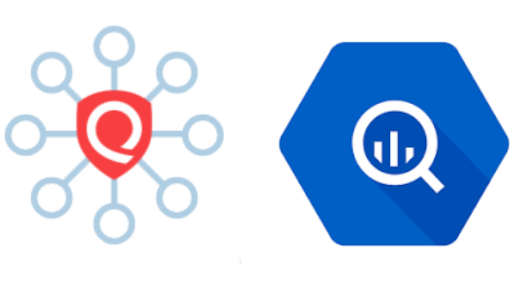


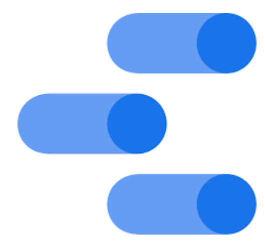


Une vision globale et à jour de l'état du parc



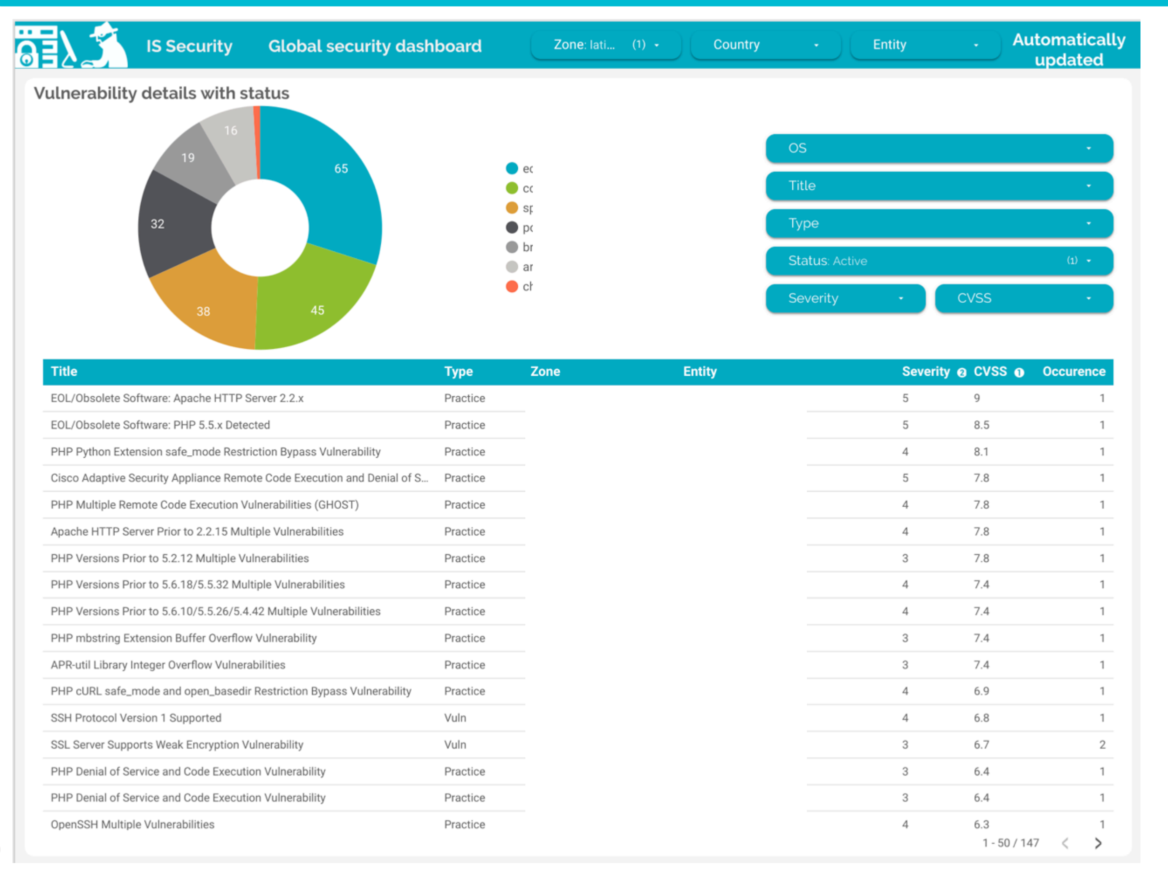




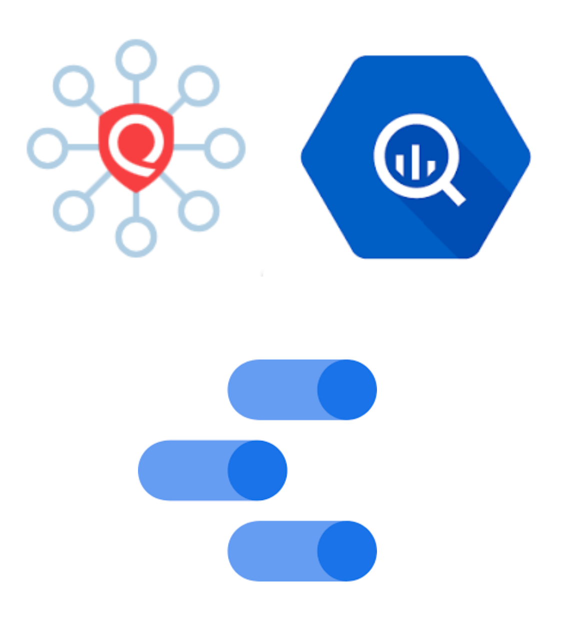


Détails sur les vulnérabilités





Title	Type	Zone	Entity	Severity	CVSS	Occurence
EOL/Obsolete Software: Apache HTTP Server 2.2.x	Practice			5	9	1
EOL/Obsolete Software: PHP 5.5.x Detected	Practice			5	8.5	1
PHP Python Extension safe_mode Restriction Bypass Vulnerability	Practice			4	8.1	1
Cisco Adaptive Security Appliance Remote Code Execution and Denial of S...	Practice			5	7.8	1
PHP Multiple Remote Code Execution Vulnerabilities (GHOST)	Practice			4	7.8	1
Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities	Practice			4	7.8	1
PHP Versions Prior to 5.2.12 Multiple Vulnerabilities	Practice			3	7.8	1
PHP Versions Prior to 5.6.18/5.5.32 Multiple Vulnerabilities	Practice			4	7.4	1
PHP Versions Prior to 5.6.10/5.5.26/5.4.42 Multiple Vulnerabilities	Practice			4	7.4	1
PHP mbstring Extension Buffer Overflow Vulnerability	Practice			3	7.4	1
APR-util Library Integer Overflow Vulnerabilities	Practice			3	7.4	1
PHP cURL safe_mode and open_basedir Restriction Bypass Vulnerability	Practice			4	6.9	1
SSH Protocol Version 1 Supported	Vuln			4	6.8	1
SSL Server Supports Weak Encryption Vulnerability	Vuln			3	6.7	2
PHP Denial of Service and Code Execution Vulnerability	Practice			3	6.4	1
PHP Denial of Service and Code Execution Vulnerability	Practice			3	6.4	1
OpenSSH Multiple Vulnerabilities	Practice			4	6.3	1



Des tendances automatisées







Perspectives 2019



- Ajout de notre politique de sécurité AWS sur CloudView
- Généralisation de l'agent sur nos assets critiques
- Intégration de nos serveurs GCP sur Qualys
- Corrélation de nos données Qualys avec notre service SOC



Questions & réponses



